IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF DELAWARE

SYMANTEC CORPORATION,	)	
	)	
Plaintiff,	)	
	)	
v.	)	C.A. No. _____
	)	
ZSCALER, INC.,	)	**JURY TRIAL DEMANDED**
	)	
Defendant.	)	

COMPLAINT FOR PATENT INFRINGEMENT

Plaintiff Symantec Corporation ("Symantec") files this complaint for patent infringement against Defendant Zscaler, Inc. ("Zscaler") and in support thereof alleges and avers as follows:

NATURE OF THE ACTION

1. This is an action for patent infringement arising under the patent laws of the United States, 35 U.S.C. § 1 *et seq*., specifically including 35 U.S.C. § 271.

THE PARTIES

2. Symantec is a corporation organized under the laws of the State of Delaware, with a principal place of business at 350 Ellis Street, Mountain View, California.

3. On information and belief, Zscaler is a corporation organized under the laws of the State of Delaware, with a principal place of business at 110 Rose Orchard Way, San Jose, California.

JURISDICTION AND VENUE

4. This Court has subject matter jurisdiction over this patent infringement action pursuant to 28 U.S.C. §§ 1331 and 1338(a).

5. Zscaler is deemed to reside in this judicial district by virtue of being incorporated in the State of Delaware. In addition, on information and belief, Zscaler regularly transacts

business in Delaware, including but not necessarily limited to offering products or services that infringe one or more of Symantec's asserted patents to customers located in Delaware and/or for use in Delaware. Accordingly, this Court may properly exercise personal jurisdiction over Zscaler.

6. Venue lies in this judicial district pursuant to 28 U.S.C. §§ 1391(b), 1391(c) and/or 1400(b) at least because Zscaler is deemed to reside in this judicial district by virtue of being incorporated in the State of Delaware. In addition, on information and belief, Zscaler has committed acts of infringement in the State of Delaware, including but not necessarily limited to offering products or services that infringe one or more of Symantec's asserted patents to customers located in Delaware and/or for use in Delaware.

THE PATENTS-IN-SUIT

7. U.S. Patent No. 6,279,113 ("the '113 Patent"), titled "Dynamic Signature Inspection-Based Network Intrusion Detection," was issued by the United States Patent and Trademark Office ("USPTO") on August 21, 2001. Symantec is the owner by assignment of the entire right, title and interest in and to the '113 Patent, including the sole and undivided right to sue for infringement. A true and correct copy of the '113 Patent is attached hereto as Exhibit A.

8. U.S. Patent No. 7,203,959 ("the '959 Patent"), titled "Stream Scanning Through Network Proxy Servers," was issued by the USPTO on April 10, 2007. Symantec is the owner by assignment of the entire right, title and interest in and to the '959 Patent, including the sole and undivided right to sue for infringement. A true and correct copy of the '959 Patent is attached hereto as Exhibit B.

9. U.S. Patent No. 7,246,227 ("the '227 Patent"), titled "Efficient Scanning of Stream Based Data," was issued by the USPTO on July 17, 2007. Symantec is the owner by

assignment of the entire right, title and interest in and to the ’227 Patent, including the sole and undivided right to sue for infringement. A true and correct copy of the ’227 Patent is attached hereto as Exhibit C.

10. U.S. Patent No. 7,392,543 (“the ’543 Patent”), titled “Signature Extraction System and Method,” was issued by the USPTO on June 24, 2008. Symantec is the owner by assignment of the entire right, title and interest in and to the ’543 Patent, including the sole and undivided right to sue for infringement. A true and correct copy of the ’543 Patent is attached hereto as Exhibit D.

11. U.S. Patent No. 7,735,116 (“the ’116 Patent”), titled “System and Method for Unified Threat Management With a Relational Rules Methodology,” was issued by the USPTO on June 8, 2010. Symantec is the owner by assignment of the entire right, title and interest in and to the ’116 Patent, including the sole and undivided right to sue for infringement. A true and correct copy of the ’116 Patent is attached hereto as Exhibit E.

12. U.S. Patent No. 8,181,036 (“the ’036 Patent”), titled “Extrusion Detection of Obfuscated Content,” was issued by the USPTO on May 15, 2012. Symantec is the owner by assignment of the entire right, title and interest in and to the ’036 Patent, including the sole and undivided right to sue for infringement. A true and correct copy of the ’036 Patent is attached hereto as Exhibit F.

13. U.S. Patent No. 8,661,498 (“the ’498 Patent”), titled “Secure and Scalable Detection of Preselected Data Embedded In Electronically Transmitted Messages,” was issued by the USPTO on February 25, 2014. Symantec is the owner by assignment of the entire right, title and interest in and to the ’498 Patent, including the sole and undivided right to sue for infringement. A true and correct copy of the ’498 Patent is attached hereto as Exhibit G.

14. The ’113 Patent, ’959 Patent, ’227 Patent, ’543 Patent, ’116 Patent, ’036 Patent and ’498 Patent are referred to herein collectively as the Patents-in-Suit.

BACKGROUND OF THE DISPUTE

Symantec Is a Pioneer in Fundamental Networking and Security Technology

15. Since its inception, Symantec has been providing software products to enhance its customers' computing productivity, security and reliability. Symantec was founded in 1982 by computer scientist Gary Hendrix with a grant from the National Science Foundation. Originally focused on natural language processing and artificial intelligence-related products, Symantec grew throughout the 1980s through organic growth and strategic acquisitions in the computer software field. In 1990, Symantec merged with Peter Norton Computing, a developer of various consumer antivirus and data management utilities. At the time, Symantec was already a market leader for Macintosh antivirus and utilities software and had already begun development of a DOS-based antivirus program, making the merger with Norton strategically advantageous. Norton AntiVirus was launched in 1991. In 1993, the Norton product group accounted for 82% of Symantec's total revenues.

16. Among other areas of expansion, Symantec sought to develop and acquire more products for corporate customers. Specifically, Symantec sought to offer products that would serve enterprise environments in which desktop computers were connected with local and other networks. Symantec was determined to achieve a goal of providing integrated, platform independent and centralized network administration solutions. Symantec’s investment and innovation led to the launching the Norton Enterprise Framework in 1996. By the late 1990s, Symantec was marketing three major product lines. The first line covered security and assistance products, consisting mainly of Norton AntiVirus and Norton Utilities products to keep personal

computers protected and reliable. The second line included remote productivity solutions, which enabled telecommuters, mobile professionals and workers in remote offices to access information, applications and data on-demand from any location. The third line included internet tools, primarily for Java programmers. Symantec expended tremendous resources in research and development to create the intellectual property upon which all of these products are based.

17. Symantec has continued its innovation, helping customers from consumers and small businesses to the largest global organizations secure and manage their information. Symantec has invested over $10 billion in research and development since 2004, and a significant portion of that investment is protected by a portfolio of over 2,000 United States patents.

Zscaler's Infringing Cloud Security Platform

18. Zscaler is a relative newcomer to the network security arena, having been founded in 2008. Zscaler has gained momentum in the marketplace through unlawful use of the technology claimed in the Patents-in-Suit. Symantec and Zscaler are direct competitors in the network security space, and Zscaler's infringement of the Patents-in-Suit is causing Symantec irreparable harm.

19. On information and belief, Zscaler's cloud security platform, including without limitation its Zscaler Enforcement Node or "ZEN" component (collectively, "the Zscaler Platform"), infringes one or more of the Patents-in-Suit, as described in more detail below.

PATENT INFRINGEMENT CLAIMS

Count I – Infringement of U.S. Patent No. 6,279,113

20. Symantec incorporates by reference the allegations in Paragraphs 1 through 19 above.

21. The ’113 Patent is generally directed to a specific method and system for detecting network intrusion attempts that includes, in some embodiments, storing corresponding data representative of a correspondence between subsets of attack signature profiles and network objects such that each network object has a corresponding stored subset of attack signature profiles and executing at least one attack signature profile included in the subset corresponding to the network object to determine if the data addressed to the network object is associated with a network intrusion attempt, among other features. *See* ’113 Patent, Abstract.

22. On information and belief, Zscaler directly infringes one or more claims of the ’113 Patent, either literally or under the doctrine of equivalents. Non-limiting examples of such infringement are provided below, based on the limited information currently available to Symantec.

23. Claim 1 of the ’113 Patent recites as follows:

> A method for detecting network intrusion attempts associated with network objects on a communications network including the steps of:
>
> storing a list of attack signature profiles descriptive of attack signatures associated with said network intrusion attempts;
>
> storing corresponding data representative of a correspondence between subsets of said attack signature profiles and said network objects such that each network object has a corresponding stored subset of attack signature profiles and more than one subset of attack signature profiles corresponds to network objects;
>
> monitoring network traffic transmitted over said communications network for data addressed to one of said network objects;
>
> in response to detecting said data addressed to said network object, accessing a subset of attack signature profiles corresponding to said network object based on said correspondence data; and
>
> executing at least one attack signature profile included in said subset corresponding to said network object to determine if said data addressed to said network object is associated with a network intrusion attempt.

24. On information and belief, the Zscaler Platform satisfies each and every limitation of at least Claim 1. The Zscaler Platform detects network intrusion attempts associated with network objects on a communications network. For example, the Zscaler Platform provides an anti-virus and anti-spyware solution to protect users from threats in web pages, emails, and files. The Zscaler Platform stores a list of attack signature profiles descriptive of attack signatures associated with the network intrusion attempts. For example, the Zscaler Platform provides a searchable threat library for storing signatures. The Zscaler Platform stores corresponding data representative of a correspondence between subsets of the attack signature profiles and the network objects such that each network object has a corresponding stored subset of attack signature profiles and more than one subset of attack signature profiles corresponds to network objects. The Zscaler Platform stores results of a Malware Detection Policy in which a user selects the type of spyware, virus, and other malware threat that the user wishes to have blocked. The Zscaler Platform also enforces firewall and web policies by location, department, group, and user. The Zscaler Platform monitors network traffic transmitted over the communications network for data addressed to one of the network objects. The Zscaler Platform inspects and enforces policies on traffic leaving an organization and coming into an organization. The Zscaler Platform, in response to detecting the data address to the network object, accesses a subset of attack signature profiles corresponding to the network object based on the correspondence, and executes at least one attack signature profile included in the subset corresponding to the network object to determine if the data addressed to the network object is associated with a network intrusion attempt. The Zscaler Platform receives web traffic for an organization and inspects the traffic and applies the signatures corresponding to the organization's policies, such as signatures that detect the type of spyware, virus, and other

malware threat that was selected to be blocked for the organization or for selected location, department, group, or user.

25. In view of the foregoing, the Zscaler Platform directly infringes the ’113 Patent in violation of 35 U.S.C. § 271(a).

26. On information and belief, both by configuring the Zscaler Platform to operate in an manner that Zscaler knows infringes the ’113 Patent and by encouraging customers to use the Zscaler Platform in a manner that Zscaler knows infringes the ’113 Patent, Zscaler is inducing infringement of the ’113 Patent by its customers in violation of 35 U.S.C. § 271(b). For example, Zscaler’s marketing literature touts functionality of the Zscaler Platform that falls within the scope of the above-identified claims of the ’113 Patent.

27. Symantec has no adequate remedy at law for Zscaler’s acts of infringement. As a direct and proximate result of Zscaler’s acts of infringement, Symantec has suffered and continues to suffer damages and irreparable harm. Unless Zscaler’s acts of infringement are enjoined by this Court, Symantec will continue to be damaged and irreparably harmed.

28. On information and belief, the ’113 Patent was brought to Zscaler’s attention during prosecution of Zscaler’s own patent (U.S. Patent No. 8,365,259), and Zscaler has been aware of that patent since at least September 18, 2012. Nevertheless, Zscaler has continued its infringement of the ‘113 Patent with full knowledge of that infringement. Zscaler’s infringement of the ’113 Patent has been willful, done deliberately and with full knowledge that the use of the Zscaler Platform infringes the ’113 Patent, justifying an increase in the damages to be awarded to Symantec up to three times the amount found or assessed, in accordance with 35 U.S.C. § 284.

29. Zscaler's willful infringement of the '113 Patent renders this an exceptional case, justifying an award to Symantec of its reasonable attorney fees, in accordance with 35 U.S.C. § 285.

Count II – Infringement of U.S. Patent No. 7,203,959

30. Symantec incorporates by reference the allegations in Paragraphs 1 through 29 above.

31. The '959 Patent is generally directed to reducing the latency in malicious code detection for computers. *See* '959 Patent, 1:6-8 and 1:46-47.

32. On information and belief, Zscaler directly infringes one or more claims of the '959 Patent, either literally or under the doctrine of equivalents. Non-limiting examples of such infringement are provided below, based on the limited information currently available to Symantec.

33. Claim 1 of the '959 Patent recites as follows:

> A method for managing transmission of a requested computer file from a remote host to a client, the method comprising the steps of:
>
> receiving a chunk of the requested computer file from the remote host;
>
> generating a hash of the chunk of the requested computer file;
>
> comparing the hash of the chunk of the requested computer file to a hash of a chunk of a previously downloaded computer file; and
>
> transmitting the chunk of the requested file to the client when the hash of the chunk of the requested computer file is identical to the hash of the chunk of the previously downloaded computer file.

34. On information and belief, the Zscaler Platform satisfies each and every limitation of at least Claim 1. The Zscaler Platform implementing Zscaler's ByteScan feature manages transmission of a requested computer file (e.g., webpages, e-mails, and files) from a remote host (e.g., a remote web server) to a client (e.g., Zscaler's customers). The Zscaler Platform manages

transmission of a requested computer file by, for example, determining whether to allow or block a requested computer file transmitted from a remote host to a Zscaler customer. Zscaler's ByteScan feature scans data that is received at the ZEN component for malicious content and is listed as one of Zscaler's five "key game changing" technologies. The Zscaler Platform receives requested data from a remote host. The Zscaler Platform receives data corresponding to a webpage that a Zscaler customer requests. The Zscaler Platform also generates hashes of a chunk of a requested computer file. For example, Zscaler employs hashing algorithms on received data, such as by hashing 1 MB of a 100 MB file. These hashing algorithms involve generation of hashes of the received data. The Zscaler Platform compares a hash of a chunk of received data to a hash of a chunk of previously-downloaded data. Zscaler compares a hash of 1 MB of received data against a hash of previously-downloaded data (e.g., data that Zscaler had previously scanned) to determine if the received data has previously been scanned. The Zscaler Platform transmits data to the customer when the hash of the requested computer file is identical to the hash of the previously-downloaded computer file. When the Zscaler Platform determines that a hash of 1 MB of a requested 100 MB computer file matches a hash of a previously-downloaded computer file, Zscaler transmits at least a portion of the requested computer file to the customer. By employing hashing algorithms to identify data that has previously been scanned, Zscaler practices the '959 Patent's claims to provide inline inspection of data at high speeds.

35. In view of the foregoing, the Zscaler Platform directly infringes the '959 Patent in violation of 35 U.S.C. § 271(a).

36. On information and belief, both by configuring the Zscaler Platform to operate in an manner that Zscaler knows infringes the '959 Patent and by encouraging customers to use the

Zscaler Platform in a manner that Zscaler knows infringes the '959 Patent, Zscaler is inducing infringement of the '959 Patent by its customers in violation of 35 U.S.C. § 271(b). For example, Zscaler's marketing literature touts functionality of the Zscaler Platform that falls within the scope of the above-identified claims of the '959 Patent.

37. Symantec has no adequate remedy at law for Zscaler's acts of infringement. As a direct and proximate result of Zscaler's acts of infringement, Symantec has suffered and continues to suffer damages and irreparable harm. Unless Zscaler's acts of infringement are enjoined by this Court, Symantec will continue to be damaged and irreparably harmed.

Count III – Infringement of U.S. Patent No. 7,246,227

38. Symantec incorporates by reference the allegations in Paragraphs 1 through 37 above.

39. The '227 Patent is generally directed to reducing latency in scanning for undesirable content by making data available to scanners in parallel. *See* '227 Patent, Abstract and 1:57-67.

40. On information and belief, Zscaler directly infringes one or more claims of the '227 Patent, either literally or under the doctrine of equivalents. Non-limiting examples of such infringement are provided below, based on the limited information currently available to Symantec.

41. Claim 28 of the '227 Patent recites as follows:

> A computer implemented method of efficiently scanning stream based data, the method comprising:
>
> a stream manager receiving data from a stream;
>
> the stream manager storing a copy of received data;
>
> the stream manager informing each of a plurality of scanners that received data is available for scanning;

the stream manager receiving requests from scanners to scan received data;

the stream manager fulfilling received requests in parallel, by making a stored copy of received data available to each scanner that requests to scan that received data; and

the stream manager maintaining a record of fulfilled requests.

42. On information and belief, the Zscaler Platform satisfies each and every limitation of at least Claim 28. The Zscaler Platform performs a computer implemented method of efficiently scanning stream based data by, for example, scanning all inbound and outbound data traffic at the Zscaler ZEN. The Zscaler Platform includes a stream manager that receives data from a stream. Zscaler's ZEN receives all inbound and outbound data traffic, such as a request for data from a remote host (e.g., Google) or a response containing a file (e.g., a webpage) from the remote host. The Zscaler Platform stores a copy of received data by, for example, placing received data (e.g., packets) in shared memory. The Zscaler Platform informs each of a plurality of scanners (e.g., antivirus engines) that received data is available for scanning. Once the Zscaler Platform places received data (e.g., packets) in memory, Zscaler signals the antivirus engines thereby informing the antivirus engines that the received data is available for scanning. The Zscaler Platform performs the stream manager receiving requests from scanners to scan received data. Zscaler receives requests from its antivirus engines to scan received data during the process of reading data from memory. The Zscaler Platform performs the stream manager fulfilling received requests in parallel. Zscaler's Single Scan, Multi-Action technology performs a single scan of received data using multiple inspection engines (such as antivirus engines, URL filtering, etc.) at the same time. Zscaler touts its Single Scan, Multi-Action technique as providing the ability to run scans in parallel thereby allowing all engines to inspect the same packets at the same time. In implementing its Single Scan Multi-Action technology, Zscaler

accesses received data stored in memory and makes that data available to the various inspection engines for scanning. The Zscaler Platform performs maintaining a record of fulfilled requests by, for example, using Zscaler's NanoLog technology to log each completed scanning transaction, including whether Zscaler's scanning technology detected malicious activity. By scanning received data in parallel using its Single Scan, Multi-Action technology, Zscaler purports to ensure no added latency and quick policy decisions.

43. In view of the foregoing, the Zscaler Platform directly infringes the '227 Patent in violation of 35 U.S.C. § 271(a).

44. On information and belief, both by configuring the Zscaler Platform to operate in an manner that Zscaler knows infringes the '227 Patent and by encouraging customers to use the Zscaler Platform in a manner that Zscaler knows infringes the '227 Patent, Zscaler is inducing infringement of the '227 Patent by its customers in violation of 35 U.S.C. § 271(b). For example, Zscaler's marketing literature touts functionality of the Zscaler Platform that falls within the scope of the above-identified claims of the '227 Patent.

45. Symantec has no adequate remedy at law for Zscaler's acts of infringement. As a direct and proximate result of Zscaler's acts of infringement, Symantec has suffered and continues to suffer damages and irreparable harm. Unless Zscaler's acts of infringement are enjoined by this Court, Symantec will continue to be damaged and irreparably harmed.

Count IV – Infringement of U.S. Patent No. 7,392,543

46. Symantec incorporates by reference the allegations in Paragraphs 1 through 45 above.

47. The ’543 Patent is generally directed to protecting computer systems by automatically detecting malicious code and preventing the spread of the malicious code. *See* ’543 Patent, Abstract.

48. On information and belief, Zscaler directly infringes one or more claims of the ’543 Patent, either literally or under the doctrine of equivalents. Non-limiting examples of such infringement are provided below, based on the limited information currently available to Symantec.

49. Claim 1 of the ’543 Patent recites as follows:

> A method comprising:
>
> detecting an attack by malicious code on a first computer system;
>
> extracting a malicious code signature from said malicious code comprising:
>
> locating a caller's address of said malicious code in a memory of said first computer system; and
>
> extracting a specific number of bytes backwards from said caller's address;
>
> creating an extracted malicious code packet including said malicious code signature; and
>
> sending said extracted malicious code packet from said first computer system to a second computer system.

50. On information and belief, the Zscaler Platform satisfies each and every limitation of at least Claim 1. The Zscaler Platform implementing Web Security and Advanced Threat Protection detects an attack by malicious code (e.g., webpages, e-mails, and files). The ZEN inspects inbound and outbound traffic and detects hidden iFrames, cross-site scripts, signs of phishing attempts, cookie stealing, and botnet communications. The Zscaler Platform extracts a malicious code signature from the malicious code. As an example, the Zscaler Platform uses

signature and heuristic technologies to inspect and protect against malicious content. The Zscaler Platform locates a caller's address of the malicious code in a memory and extracts a specific number of bytes backwards from the caller's address. In extracting the malicious code signature, the ZEN component locates the malicious code and extracts a portion of the malicious code. The Zscaler Platform correlates the detected threat with information included in web traffic logs. The Zscaler Platform creates an extracted malicious code packet including the malicious code signature. By hashing the malicious code, the ZEN component creates an extracted malicious code packet that includes the malicious code packet signature. The Zscaler Platform sends the extracted malicious code packet from a first computer system to a second computer system. The ZEN component that detects the malicious code propagates a hash of the malicious code to all ZENs throughout the cloud, which allows the Zscaler Platform to block the threat for other users each time a threat is identified.

51. In view of the foregoing, the Zscaler Platform directly infringes the '543 Patent in violation of 35 U.S.C. § 271(a).

52. On information and belief, both by configuring the Zscaler Platform to operate in an manner that Zscaler knows infringes the '543 Patent and by encouraging customers to use the Zscaler Platform in a manner that Zscaler knows infringes the '543 Patent, Zscaler is inducing infringement of the '543 Patent by its customers in violation of 35 U.S.C. § 271(b). For example, Zscaler's marketing literature touts functionality of the Zscaler Platform that falls within the scope of the above-identified claims of the '543 Patent.

53. Symantec has no adequate remedy at law for Zscaler's acts of infringement. As a direct and proximate result of Zscaler's acts of infringement, Symantec has suffered and

continues to suffer damages and irreparable harm. Unless Zscaler's acts of infringement are enjoined by this Court, Symantec will continue to be damaged and irreparably harmed.

54. On information and belief, the '543 Patent was brought to Zscaler's attention during prosecution of Zscaler's own patent and patent application (U.S. Patent No. 9,152,789 and U.S. Patent Appln. Publication No. 2015/0319182), and Zscaler has been aware of that patent since at least May 19, 2015. Nevertheless, Zscaler has continued its infringement of the '543 Patent with full knowledge of that infringement. Zscaler's infringement of the '543 Patent has been willful, done deliberately and with full knowledge that the use of the Zscaler Platform infringes the '543 Patent, justifying an increase in the damages to be awarded to Symantec up to three times the amount found or assessed, in accordance with 35 U.S.C. § 284.

55. Zscaler's willful infringement of the '543 Patent renders this an exceptional case, justifying an award to Symantec of its reasonable attorney fees, in accordance with 35 U.S.C. § 285.

Count V – Infringement of U.S. Patent No. 7,735,116

56. Symantec incorporates by reference the allegations in Paragraphs 1 through 55 above.

57. The '116 Patent is generally directed to a threat management system that efficiently allocates computing resources and reduces packet processing latencies by performing security tests according to a security hierarchy. *See* '116 Patent, Abstract.

58. On information and belief, Zscaler directly infringes one or more claims of the '116 Patent, either literally or under the doctrine of equivalents. Non-limiting examples of such infringement are provided below, based on the limited information currently available to Symantec.

59. Claim 1 of the '116 Patent recites as follows:

> A method of controlling access to a networked device, the method comprising:
>
> receiving an incoming message packet by a security gateway coupled to said networked device;
>
> evaluating the received message packet to determine if the received message packet is compliant with a first test, the first test corresponding to a first level of a security hierarchy implemented by said security gateway, wherein the security hierarchy establishes a relationship between security functions from a lowest level to a highest level; and the received packet is rejected at the earliest possible operation in the processing of the packet in the security hierarchy;
>
> forwarding the received packet and an indication of its compliance with the first test for subsequent processing upon the received packet complying with the first test; and
>
> dropping the received packet whereby no further processing of the received packet is performed upon the received packet not complying with the first test.

60. On information and belief, the Zscaler Platform satisfies each and every limitation of at least Claim 1. The Zscaler Platform receives an incoming message packet (e.g., webpage, email, or file) using a security gateway (e.g., ZEN) coupled to a networked device (e.g., Zscaler's customers, content providers, or Internet-connected devices). The Zscaler Platform evaluates the received message packet according to a security hierarchy. As an example, the Zscaler Platform inspects incoming content according to levels that, from lowest level to highest level, include: destination analysis, antivirus/antispyware inspection, full content inspection, browser control, and interrogator cloud mining. The Zscaler Platform evaluates a first test, such as the destination analysis test. The Zscaler Platform rejects the received packet at the earliest possible operation in the processing of the packet in the security hierarchy. In particular, Zscaler subjects content to each level of inspection unless malicious content is definitively identified at a

lower level. Thus, if the received packet complies with the first test (e.g., destination analysis), the received packet and an indication of its compliance with the first test is sent for subsequent processing by a higher level of the hierarchy (e.g., antivirus/antispyware inspection). If the received packet does not comply with the first test (e.g., destination analysis), the received packet is dropped without further processing by the subsequent levels of the hierarchy. For example, Zscaler's destination analysis test provides the most basic level of protection, leveraged to quickly filter out known malicious content without the need for deeper inspection by the higher levels. More generally, the Zscaler Platform processes rules in order (e.g., first rule 1, then rule 2, followed by rule 3, and so on). After a rule's condition has been met, the Zscaler Platform does not process subsequent rules. Thus, Zscaler practices at least the '116 Patent's claims to processing a packet according to a security hierarchy and rejecting the packet at the earliest possible operation of the security hierarchy.

61. In view of the foregoing, the Zscaler Platform directly infringes the '116 Patent in violation of 35 U.S.C. § 271(a).

62. On information and belief, both by configuring the Zscaler Platform to operate in an manner that Zscaler knows infringes the '116 Patent and by encouraging customers to use the Zscaler Platform in a manner that Zscaler knows infringes the '116 Patent, Zscaler is inducing infringement of the '116 Patent by its customers in violation of 35 U.S.C. § 271(b). For example, Zscaler's marketing literature touts functionality of the Zscaler Platform that falls within the scope of the above-identified claims of the '116 Patent.

63. Symantec has no adequate remedy at law for Zscaler's acts of infringement. As a direct and proximate result of Zscaler's acts of infringement, Symantec has suffered and

continues to suffer damages and irreparable harm. Unless Zscaler's acts of infringement are enjoined by this Court, Symantec will continue to be damaged and irreparably harmed.

Count VI – Infringement of U.S. Patent No. 8,181,036

64. Symantec incorporates by reference the allegations in Paragraphs 1 through 63 above.

65. The '036 Patent is generally directed to techniques that enable extrusion detection even if confidential information is encrypted, compressed, or otherwise obfuscated before transmission. *See* '036 Patent, Abstract.

66. On information and belief, Zscaler directly infringes one or more claims of the '036 Patent, either literally or under the doctrine of equivalents. Non-limiting examples of such infringement are provided below, based on the limited information currently available to Symantec.

67. Claim 1 of the '036 Patent recites as follows:

> A computer-implemented method for detecting extrusion of obfuscated content, comprising:
>
> comparing signatures of programs launched on a computer with signatures of known obfuscation tools;
>
> detecting launching of an obfuscation tool on the computer responsive to a signature of a program launched on the computer matching a signature of a known obfuscation tool;
>
> responsive to detecting launching of the obfuscation tool, determining if a file being opened by the obfuscation tool is classified as sensitive, the determining comprising:
>
> determining if the file contains a word/phrase indicative of sensitive information;
>
> responsive to determining that the file contains the word/phrase indicative of sensitive information, interrogating the file to glean a context in which the word/phrase is used; and

determining whether the file is classified as sensitive responsive to results of the interrogation;

responsive to a determination that the file being opened by the obfuscation tool is classified as sensitive, determining that the obfuscation tool produces an output file and classifying the output file as sensitive;

computing a signature of the output file; and

using the signature of the output file to prevent extrusion of obfuscated sensitive content within the output file.

68. On information and belief, the Zscaler Platform satisfies each and every limitation of at least Claim 1. The Zscaler Platform compares signatures of programs launched on a computer with signatures of known obfuscation tools and detects launching of an obfuscation tool on the computer responsive to a signature of a program launched on the computer matching a signature of the known obfuscation tool. The Zscaler Platform inspects traffic and detects SSL-encrypted or compressed traffic in real time. Responsive to detecting launching of the obfuscation tool, the Zscaler Platform determines if a file being opened by the obfuscation tool is classified as sensitive. In particular, the Zscaler Platform determines if the file contains a word/phrase indicative of sensitive information. The Zscaler Platform's Data Loss Prevention ("DLP") service uses DLP dictionaries to identify protected content, including special dictionaries that identify a specific type of number or content type (e.g., credit card and/or social security numbers), Artificial Intelligence (AI) engine based dictionaries that identify types of documents, and phrase based dictionaries that use fuzzy matching techniques to ensure phrases match regardless of capitalization, spacing and noise words.

69. Responsive to a determination that the file contains the word/phrase indicative of sensitive information, the Zscaler Platform interrogates the file to glean a context in which the word/phrase is used, and determines whether the file is classified as sensitive responsive to

results of the interrogation. The Zscaler Platform uses a confidence score threshold to minimize the number of false positives generated by the dictionaries. As one example, the Zscaler Platform will determine that a file is classified as sensitive if its content matches a valid range, is in a popular format, and is accompanied by keywords such as "date of birth," "social security number," "tax payer id," and "password."

70. Responsive to a determination that the file being opened is classified as sensitive, the Zscaler Platform determines that the obfuscation tool produces an output file and classifies the output file as sensitive, computes a signature of the output file, and uses the signature of the output file to prevent extrusion of obfuscated sensitive content within the output file. The Zscaler Platform uses inline scanning to log or block transactions with confidential data. The Zscaler Platform's integrated DLP service uses a single policy to scan across web and email traffic, and changes are instantly reflected across the entire cloud. Thus, Zscaler practices at least the '036 Patent's claims to detecting extrusion of obfuscated content.

71. In view of the foregoing, the Zscaler Platform directly infringes the '036 Patent in violation of 35 U.S.C. § 271(a).

72. On information and belief, both by configuring the Zscaler Platform to operate in an manner that Zscaler knows infringes the '036 Patent and by encouraging customers to use the Zscaler Platform in a manner that Zscaler knows infringes the '036 Patent, including for example by encouraging customers to use the Zscaler Platform in connection with external DLP engines for scanning content to protect against loss of sensitive data, Zscaler is inducing infringement of the '036 Patent by its customers in violation of 35 U.S.C. § 271(b). For example, Zscaler's marketing literature touts functionality of the Zscaler Platform that falls within the scope of the above-identified claims of the '036 Patent.

73. Symantec has no adequate remedy at law for Zscaler's acts of infringement. As a direct and proximate result of Zscaler's acts of infringement, Symantec suffered and continues to suffer damages and irreparable harm. Unless Zscaler's acts of infringement are enjoined by this Court, Symantec will continue to be damaged and irreparably harmed.

Count VII – Infringement of U.S. Patent No. 8,661,498

74. Symantec incorporates by reference the allegations in Paragraphs 1 through 73 above.

75. The '498 Patent is generally directed to a system for detecting preselected data embedded in electronically transmitted messages to prevent the escape of (or log) messages that contain sensitive information. *See* '498 Patent, Abstract and 4:60-5:2.

76. On information and belief, Zscaler directly infringes one or more claims of the '498 Patent, either literally or under the doctrine of equivalents. Non-limiting examples of such infringement are provided below, based on the limited information currently available to Symantec.

77. Claim 1 of the '498 Patent recites as follows:

> A method comprising:
>
> identifying, by a message monitoring system (MMS), an abstract data structure derived from preselected data to be protected from traveling across a network, the abstract data structure not revealing data elements of the preselected data to be protected;
>
> performing, by the MMS, content searches on a plurality of messages electronically transmitted to reach a respective destination over the network, the content searches to be performed to determine whether one or more of the plurality of searched messages contain at least a portion of the preselected data to be protected using the abstract data structure that does not reveal the data elements of the preselected data; and
>
> causing a searched message of the plurality of searched messages to be prevented from reaching the respective destination in response to a determination

that the searched message contains at least a portion of the preselected data to be protected.

78. On information and belief, the Zscaler Platform satisfies each and every limitation of at least Claim 1. The Zscaler Platform identifies, using a message monitoring system (e.g., the Zscaler Platform and, in particular, the integrated DLP service), an abstract data structure derived from preselected data to be protected from traveling across a network. As an example, Zscaler's DLP engines implement DLP rules using DLP dictionaries that identify specific types of information such as numbers (e.g., credit card or social security numbers) or content type, and AI engine based dictionaries that identify types of documents to be protected. The Zscaler Platform performs content searches on a plurality of messages electronically transmitted to reach a respective destination over the network to determine whether one or more of the plurality of searched messages contain at least a portion of the preselected data to be protected using the abstract data structure. The Zscaler Platform scans data leaving an organization for potential data loss, including credit cards and social security numbers using the DLP dictionaries. The Zscaler Platform causes a searched message of the plurality of searched messages to be prevented from reaching the respective destination in response to a determination that the searched message contains at least a portion of the preselected data to be protected. Zscaler's DLP engines detect and allow or block transactions that trigger DLP rules to protect against the loss of sensitive data (e.g., credit card numbers, social security numbers, and other data). Thus, Zscaler practices at least the '498 Patent's claims to performing content searches on electronically transmitted messages and causing searched messages to be prevented from reaching their destination if the searched message contains a portion of preselected data to be protected.

79. In view of the foregoing, the Zscaler Platform directly infringes the '498 Patent in violation of 35 U.S.C. § 271(a).

80. On information and belief, both by configuring the Zscaler Platform to operate in an manner that Zscaler knows infringes the '498 Patent and by encouraging customers to use the Zscaler Platform in a manner that Zscaler knows infringes the '498 Patent, including for example by encouraging customers to use the Zscaler Platform in connection with external DLP engines for scanning content to protect against loss of sensitive data, Zscaler is inducing infringement of the '498 Patent by its customers in violation of 35 U.S.C. § 271(b). For example, Zscaler's marketing literature touts functionality of the Zscaler Platform that falls within the scope of the above-identified claims of the '498 Patent.

81. Symantec has no adequate remedy at law for Zscaler's acts of infringement. As a direct and proximate result of Zscaler's acts of infringement, Symantec suffered and continues to suffer damages and irreparable harm. Unless Zscaler's acts of infringement are enjoined by this Court, Symantec will continue to be damaged and irreparably harmed.

PRAYER FOR RELIEF

WHEREFORE, Symantec prays for judgment in their favor granting the following relief:

A. A finding that Zscaler has directly infringed and/or induced others to infringe the Patents-in-Suit;

B. An award of damages pursuant to 35 U.S.C. § 284 adequate to compensate Symantec for Zscaler's infringement of the Patents-in-Suit, including both pre- and post-judgment interest and costs as fixed by the Court;

C. A preliminary and/or permanent injunction against Zscaler and its officers, agents, servants, employees, and representatives, and all others in active concert or participation with them, from further infringing the Patents-in-Suit;

D. A finding that Zscaler's infringement of at least the '113 Patent and '543 Patent has been willful;

E. An increase in the damages to be awarded to Symantec of three times the amount found by the jury or assessed by the Court;

F. A declaration that this is an exceptional case within the meaning of 35 U.S.C. § 285, and a corresponding award of Symantec's reasonable attorney fees incurred in connection with the litigation; and

G. Any additional and further relief the Court may deem just and proper under the circumstances.

JURY DEMAND

Pursuant to Federal Rule of Civil Procedure 38(b) and District of Delaware Local Rule 38.1, Plaintiff hereby demands a trial by jury on all issues so triable.

MORRIS, NICHOLS, ARSHT & TUNNELL LLP

/s/ Jack B. Blumenfeld

Jack B. Blumenfeld (#1014)
1201 North Market Street
P.O. Box 1347
Wilmington, DE 19899-1347
(302) 658-9200
jblumenfeld@mnat.com

Attorneys for Plaintiff Symantec Corporation

OF COUNSEL:

Kurt Pankratz
Chad Walters
BAKER BOTTS LLP
2001 Ross Avenue
Dallas, TX 75201
(214) 953-6500

Jennifer C. Tempesta
BAKER BOTTS LLP
30 Rockefeller Plaza
New York, NY 10112
(212) 408-2571

December 12, 2016